



DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MEDICAL DEPARTMENT CENTER AND SCHOOL
AND FORT SAM HOUSTON
2250 STANLEY ROAD
FORT SAM HOUSTON, TEXAS 78234-6100

REPLY TO
ATTENTION OF:

08 FEB 2005

MCCS-BIM

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Installation Information Management (IM) Policy 25-14, Acceptable Use Policy (AUP)

1. REFERENCES.

- a. AR 25-2, Information Assurance, 14 November 2003.
- b. IMA Letter, SFIM-SW-ZA, 19 November 2004, Subject: Acceptable Use Policy for Using Army Information Systems.

2. PURPOSE. To ensure installation compliance with Army policy to safeguard Army Information Systems and Army resources.

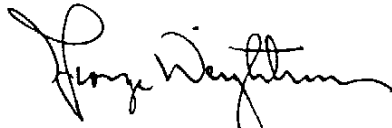
3. SCOPE. This policy applies to all organizations and units located on or supported by Fort Sam Houston (FSH), Camp Bullis, and Camp Stanley, and that have connectivity to the Installation network managed by the Directorate of Information Management (DOIM). This policy applies to Government-owned and leased automation equipment.

4. BACKGROUND. AR 25-2 requires that commanders develop and publish an Acceptable Use Policy (AUP) for all users of the installation network. Network users are advised that there is no expectation of privacy while using Army Information Systems or accessing Army resources. Recent intrusions to the network introducing viruses such as botNET, coupled with use of prohibited software such as Peer-to-Peer (P2P), indicate the need for AUPs at all Army installations.

5. POLICY. I have charged the DOIM with tracking compliance of this regulatory requirement. All users accessing Army Information Systems or Army resources have the primary responsibility to safeguard information from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use in accordance with AR 25-2. Users will agree, through signature on the attached policy, to follow the minimum security rules and requirements described. Refusal to sign the require AUP will result in denied access to the Fort Sam Houston network.

6. This policy will be reviewed 1 year from date of publication.

7. Point of contact is Ms. Cynthia S. Helton, Director of Information Management, telephone (210) 221-1300, or email cynthia.helton@us.army.mil.



GEORGE W. WEIGHTMAN
Major General, MC
Commanding

Encl

DISTRIBUTION:
A

Acceptable Use Policy
FORT SAM HOUSTON LOCAL AREA NETWORK And DoD NIPRNet
December 2004

1. **Understanding.** I have the primary responsibility to safeguard the information contained in the Fort Sam Houston (FSH) Local Area Network (LAN) and by extension, the Department of Defense Non-classified Internet Protocol Network (NIPRNet) from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use in accordance with AR 25-2.
2. **Access.** Access to these networks is for official use and authorized purposes and as set forth in DoD 5500.7-R, "Joint Ethics Regulation" or as further limited by this policy.
3. **Revocability.** Access to Army resources is a revocable privilege and subject to content monitoring and security testing.
4. **Unclassified information processing.** The NIPRNet is the primary unclassified information system for the organizations and personnel assigned to Fort Sam Houston.
 - a. The NIPRNet provides unclassified communication to external DoD and other United States Government organizations. This is done via electronic mail and Internet working protocols such as web, ftp, telnet, etc.
 - b. The NIPRNet is approved to process UNCLASSIFIED, SENSITIVE information.
 - c. The NIPRNet and the Internet as viewed by the Commander, AMEDDC&S and Fort Sam Houston are synonymous. E-Mail and attachments to E-mail are vulnerable to interception as they traverse the NIPRNet and the Internet.
5. **Minimum-security rules and requirements.** As a NIPRNet system user, the following minimum security rules and requirements apply:
 - a. Personnel are not permitted access to the NIPRNet unless in compliance with AR 25-2.
 - b. I have completed the user security awareness-training module. I will participate in all training programs as required (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before receiving system access.
 - c. I will generate and protect password or pass-phrases. Passwords will consist of at least 10 characters with 2 each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this account. I will not use my user ID, common names, birthdays, phone numbers, military acronyms, call signs, or dictionary based words as password or pass-phrases.
 - d. I understand that I am responsible for any and all activity that occurs under my assigned USERID. I will not reveal my individual password to anyone. I will not store my password on any processor, microcomputer, magnetic, or electronic media - unless such storage is approved in writing by the DOIM.
 - e. I will use only authorized hardware and software. I will not download, install or use any personally owned hardware, software, shareware, or public domain software on a government owned computer without prior approval of the DOIM.

Acceptable Use Policy
FORT SAM HOUSTON LOCAL AREA NETWORK And DoD NIPRNet
December 2004

- f. I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, compact disk, or web site.
- g. I will not attempt to access or process data exceeding my authorized Information Security classification level. Computers connected to the NIPRNet are not authorized for the use of classified information.
- h. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized.
- i. I will not introduce executable code, i.e. .exe, .com, .vbs, or .bat files, without authorization, nor will I write malicious code.
- j. I will safeguard and mark with the appropriate classification level/ handling marking all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.
- k. I will not utilize Army or DoD provided Information Systems for commercial or financial gain or illegal activities.
- l. A System Administrator or an authorized technician will perform all maintenance.
- m. I will use screen locks or an authorized, password protected screensaver, set to activate automatically after ten minutes or less of inactivity. If I leave my workstation area for short periods (e.g., work break or restroom visit), I will log off the workstation, or ensure that I activate the Lock Computer feature to protect my workstation from unauthorized access/use during my absence.
- n. I will immediately report any suspicious output, files, shortcuts, links, or system problems to the DOIM Help Desk and cease all activities on the system.
- o. I will address any questions regarding acceptable use or information assurance to the Fort Sam Houston DOIM Security Division.
- p. I understand that each Information System, computer or network is the property of the Army. It is provided to me for official and authorized uses, is subject to monitoring for security purposes and to ensure that use is authorized, and I should not store data on the Information System that I do not want others to see.
- q. I understand that monitoring of the Fort Sam Houston Network will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution. I do not have a recognized expectation of privacy in official data on the Information System and may have only a limited expectation of privacy in personal data on the Information System.
- r. I understand that the following examples of activity define some unacceptable uses of an Army Information System:
 - The use of hacker or hacker related software on any system.
 - The intentional introduction of a virus, worm, or a Trojan horse on any computer or network.
 - The intentional breaking into, damage, defacing, or destruction of any hardware or software system belonging to another person, activity, agency, or entity.
 - Accessing internet sites oriented to pornographic or sexually based material.
 - Accessing gambling related sites is prohibited.

Acceptable Use Policy
FORT SAM HOUSTON LOCAL AREA NETWORK And DoD NIPRNet
December 2004

- Accessing, downloading, or copying of copyright protected software, literature, or music.
 - s. Activities such as the following are considered acceptable use IAW FSH Policy 25-1
 - During duty hours
 - 1. Checking in with spouse or minor children.
 - 2. Scheduling medical/dental appointments.
 - During lunch/non-duty hours/break periods
 - 1. Arranging for home/auto repairs.
 - 2. Brief visits/searches to acceptable Internet sites for personal use.
 - t. The storage or transmission of personal medical data or privacy act material without proper encryption or other safeguards is prohibited.
 - u. E-mail use and restrictions. The following are considered unauthorized use of e-mail.
 - Create, download, store, copy, transmit, or broadcast chain letters.
 - "Spam", that is, to exploit list servers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited e-mail.
 - Broadcast unsubstantiated virus warnings or messages from sources other than approved DOIM, DA, or DoD sources.
 - Broadcast e-mail messages to large groups of e-mail users (entire organizations) instead of targeting smaller specifically interested populations.
6. I understand that I may be subject to disciplinary action for any violation or abuse of access privileges.
7. The authority for soliciting your social security number (SSN) is Executive Order 939. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of this information is voluntary; however, failure to disclose the information could result in denial of access to the Fort Sam Houston Information Systems.
8. **Acknowledgement.** I have read the above requirements regarding use of the Fort Sam Houston Information Systems. I understand my responsibilities regarding these systems and the information contained in them.

Directorate/Division/Branch

Date

Last Name, First Name, MI

Rank/Grade SSN

Signature

Phone Number